



Vendor: Isaca

Exam Code: AAIR

Exam Name: Advanced in AI Risk (AAIR)

Version: DEMO

QUESTION 1

An organization uses multiple external data sources to train its AI models. Which of the following is the risk practitioner's BEST recommendation to protect the organization from data poisoning attacks?

- A. Data integrity reviews in response to indications that significant model drift has occurred
- B. Continuous monitoring and anomaly detection for data ingestion pipelines
- C. Stringent controls over model code and deployment artifacts
- D. Enhanced regularization and training techniques to limit the influence of anomalies

Answer: B

Explanation:

Continuous monitoring and anomaly detection for data ingestion pipelines provide proactive protection against data poisoning attacks by identifying suspicious, manipulated, or abnormal data before it is incorporated into model training. This directly addresses the primary attack surface created by multiple external data sources.

QUESTION 2

Which of the following poses the GREATEST challenge when performing root cause analysis for incidents involving AI systems and data?

- A. Lack of transparency
- B. Unclear system objectives
- C. Automation bias
- D. Privacy compliance

Answer: A

Explanation:

Lack of transparency is the greatest challenge because many AI systems, especially complex models, operate as "black boxes," making it difficult to trace how specific inputs, model behaviors, or decision pathways led to an incident. This significantly complicates effective root cause analysis and remediation efforts.

QUESTION 3

An organization uses AI to generate procedure documents for operational processes. Which of the following would be of GREATEST concern to a risk practitioner?

- A. AI-generated procedure documents do not undergo human review.
- B. AI-generated procedure manuals include outdated procedures.
- C. The procedures are not aligned to organizational policy.
- D. The AI model is used to generate procedures for high-risk activities.

Answer: A

Explanation:

The greatest concern is the absence of human review because AI-generated operational procedures may contain inaccuracies, unsafe instructions, hallucinations, or incomplete guidance that could directly affect operational effectiveness and control reliability. Human oversight is critical to validate accuracy, appropriateness, and compliance before procedures are implemented.

QUESTION 4

An election oversight body is considering the use of AI to identify irregularities in voting patterns. Which of the following is the MOST important risk to evaluate?

- A. Identification of voter locations
- B. Amplification of biases in historical data
- C. Susceptibility to contextual drift
- D. Distrust of AI among political interest groups

Answer: B

Explanation:

Biases in historical voting or demographic data can be amplified by AI systems, leading to unfair or discriminatory identification of irregularities and potentially undermining election integrity. Evaluating and mitigating bias is therefore the most critical risk in this context because of the significant societal, legal, and democratic impacts involved.

QUESTION 5

A risk practitioner assesses a new AI system and determines that the risk is within the organization's risk tolerance. Which of the following is the BEST recommendation to ensure system controls remain effective over time?

- A. Alignment with recognized AI control frameworks
- B. Ongoing AI security and risk awareness training
- C. Continuous monitoring for data and performance drift
- D. Periodic regulatory compliance reviews

Answer: C

Explanation:

Continuous monitoring for data and performance drift is the best recommendation because AI systems can degrade over time as data patterns, operational environments, or user behaviors change. Ongoing monitoring helps ensure controls remain effective and enables timely detection and remediation of emerging risks.

QUESTION 6

An organization plans to deploy an AI system that ingests multiple sources with varying completeness and accuracy. Which of the following is the risk practitioner's BEST recommendation?

- A. Use synthetic data augmentation to supplement training and testing.
- B. Perform post-implementation assessments to identify data integrity issues.
- C. Implement continuous real-time quality assurance (QA) processes.
- D. Fine-tune model parameters to accommodate variable inputs.

Answer: C

Explanation:

Continuous real-time quality assurance processes are the best recommendation because they directly address the ongoing risks associated with ingesting data from multiple sources with inconsistent completeness and accuracy. Real-time QA enables early detection and correction of data quality issues before they negatively affect model performance, reliability, or decision-making outcomes.

QUESTION 7

Which of the following BEST mitigates risk associated with evasion attacks on AI models?

- A. API rate limiting
- B. Anomaly detection
- C. Predictive analytics
- D. Feature importance weighting

Answer: B

Explanation:

Anomaly detection best mitigates evasion attacks because it helps identify unusual, manipulated, or adversarial inputs designed to deceive the AI model into producing incorrect outputs. Detecting abnormal behavior in inputs or model responses enables organizations to respond to potential attack activity before significant harm occurs.

QUESTION 8

An organization uses an AI model that learns from live data streams. Which of the following is the BEST course of action to manage the risk of an adaptive model?

- A. Utilize a defense-in-depth control approach for model access.
- B. Restrict data sources and perform periodic data quality inspections.
- C. Apply dynamic performance thresholds and conduct scheduled recalibrations.
- D. Implement automated monitoring to detect data drift and data poisoning.

Answer: D

Explanation:

Automated monitoring for data drift and data poisoning is the best approach because adaptive models continuously learn from live data streams and are therefore highly susceptible to changes in data patterns and malicious manipulation. Continuous monitoring enables timely detection of degraded model behavior and compromised training data before significant operational impact occurs.

QUESTION 9

A manufacturing organization has implemented an autonomous navigation system for warehouse operations. Which of the following should a risk practitioner regard as the MOST significant concern?

- A. The system is unable to learn from complex situations not encountered during training.
- B. The deep neural network used by the system contains datasets with proprietary information.
- C. The system is used to accelerate just-in-time warehouse processes.
- D. The organization uses outside contractors to address the lack of in-house AI knowledge.

Answer: A

Explanation:

The inability of the autonomous navigation system to respond appropriately to complex situations not encountered during training presents the most significant risk because it can directly affect operational safety, navigation reliability, and physical warehouse operations. Unpredictable real-world scenarios can lead to accidents, disruptions, or unsafe decisions by the AI system.

QUESTION 10

A risk practitioner is concerned that an AI model's responses have become more inaccurate over time, leading to diminished customer trust. Which of the following should the risk practitioner

recommend be done FIRST?

- A. Revise validation processes to add more review cycles.
- B. Take the model offline and perform a full backup.
- C. Fully retrain the model with a more recent dataset.
- D. Determine the impact on critical features and model outputs.

Answer: D

Explanation:

Determining the impact on critical features and model outputs should be done first because effective risk management begins with understanding the scope, severity, and business impact of the degradation. Assessing the affected outputs and functionality enables informed decisions about remediation, retraining, validation, or operational response.

QUESTION 11

Which of the following BEST helps to ensure AI model outputs can be reproduced in other environments?

- A. Requiring manual review of outputs for stability and accuracy
- B. Capturing and archiving complete snapshots of training datasets
- C. Maintaining continuous post-deployment performance monitoring
- D. Implementing AI-specific change management processes

Answer: B

Explanation:

Capturing and archiving complete snapshots of training datasets is essential for reproducibility because model outputs are heavily dependent on the exact data used during training. Preserving the original datasets enables consistent retraining, validation, and replication of model behavior across different environments and time periods.

QUESTION 12

Which of the following is the MOST important consideration when managing changes to an AI model in production?

- A. Allowing operational teams to adjust configuration parameters for real-time performance tuning
- B. Implementing stringent approval processes for user access to new model functionalities
- C. Conducting rigorous validation to assess effects on predictive accuracy and model bias
- D. Expediting rollout of changes in production to ensure service continuity and minimize downtime

Answer: C

Explanation:

Rigorous validation is the most important consideration because changes to an AI model can introduce unintended effects on predictive accuracy, fairness, reliability, and bias. Thorough testing and validation ensure the updated model continues to operate safely and effectively before deployment into production.

QUESTION 13

Which of the following is the GREATEST benefit of incorporating AI technology for data asset management?

- A. Justifying the use of synthetic data to augment smaller datasets

- B. Reducing the initial impacts of data poisoning and exfiltration attacks
- C. Providing more rapid identification of overfitting during model training
- D. Automating data cleaning and metadata tagging for large datasets

Answer: D

Explanation:

Automating data cleaning and metadata tagging provides the greatest benefit for data asset management because AI can efficiently process and organize large volumes of data, improving data quality, consistency, discoverability, and usability while reducing manual effort and operational overhead.

QUESTION 14

A risk practitioner is performing a post-implementation review for an AI system used for credit scoring. Which of the following is MOST important for the risk practitioner to confirm?

- A. Access token runtime is logged and timestamped.
- B. The AI system's decisions are explainable and fair.
- C. Performance metrics are frequently communicated to stakeholders.
- D. Employees find the AI system easy to learn and use.

Answer: B

Explanation:

For an AI system used in credit scoring, it is most important to confirm that decisions are explainable and fair because the system directly affects individuals' financial opportunities and may be subject to regulatory, ethical, and discrimination concerns. Explainability and fairness are critical to ensuring transparency, accountability, and equitable outcomes.

QUESTION 15

A credit-scoring AI solution exhibits steadily declining accuracy despite unchanged input distributions. Which of the following should a risk practitioner consider to be the GREATEST risk?

- A. Technical delays affecting credit score updates
- B. Underfitting resulting from shortened training cycles
- C. Concept drift leading to faulty decisions
- D. Increased model retraining costs

Answer: C

Explanation:

Concept drift is the greatest risk because declining model accuracy despite stable input distributions indicates that the relationship between inputs and expected outcomes has changed over time. In a credit-scoring context, this can lead to faulty lending decisions, unfair outcomes, and increased regulatory and operational risk.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



10% Discount Coupon Code: ASTR14